Complying with HIPAA: The Challenge for HCAP Grantees

Presented by Michael B. Glomb, Esq.

Feldesman Tucker Leifer Fidell LLP
2001 L Street, NW Washington, DC 20036
(202) 466-8960 www.feldesmantucker.com

HIPAA Components

- **Privacy Rule (April 14, 2003)**
- **Electronic Transmission and Code Sets (October 16, 2003)**
- **Security Rule (April 21, 2005)**

Purpose

- **The Privacy Rule sets a federal "floor" regarding patient privacy**
- **It does not preempt state laws with stricter standards**
- **Stricter federal laws take precedence**

Purpose

- **What is a stricter standard?**
  - **Law provides greater patient access to protected health information ("PHI")**
  - **Law contains greater restrictions on use or disclosure of PHI**

Purpose

- **The Electronic Transmission and Code Sets standards implement mandatory standards for processing HIPAA-covered transactions**

Key Features

- **HIPAA-covered transactions:**
  - **health claims or equivalent encounter information**
  - **health care payment and remittance advice**
  - **enrollment and disenrollment in a health plan**
  - **eligibility for a health plan**
  - **health plan premium payments**

Key Features

- **HIPAA-covered transactions:**
  - **first report of injury**
  - **health care claim status**
  - **referral certification and authorization**
  - **health claims attachments**
  - **coordination of benefits**

Purpose

- **The Security Rule standard mandates requirements for electronic transmission of PHI**

Key Features

- **Who is covered?**
  - ***Health care providers*** **– providers of medical or health services (as defined by Medicare) and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business**

Key Features

- ***Health plans*** **– individual or group plans that provide, or pay the cost of, medical care. Includes Medicare, Medicaid, group health plans, CHAMPUS, FEHBP, active military, veterans, *etc*.**

Key Features

- ***Health care clearinghouses*** **– entities that process or facilitate the processing of standard and nonstandard health data content and elements that transmit information electronically in connection with a HIPAA-covered transaction**

Key Features

- **What kind of information is covered?**
  - ***Health information*** **B any information that is created or received by a health care provider that relates to:**
    - **the past, present, or future physical or mental health or condition of an individual**
    - **the provision of health care to an individual**
    - **the past, present or future payment for the provision of health care to an individual**

Key Features

- ***Individually identifiable*** B **information that identifies an individual or for which there is a reasonable basis to believe that the information can be used to identify the individual, including demographic information**

Key Features

- **Privacy Rule covers PHI in any form – *i.e.*, electronic, oral, or paper (written)**
- **Security Rule applies to electronic transmission of PHI**

Key Features

- **What activities are covered by HIPAA?**
  - ***Use*** **– the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information**
  - ***Disclosure*** **– the release, transfer, provision of access to, or the divulging in any other manner of information outside the entity holding the information**

Covered Entity Obligations

- **A covered entity must disclose PHI in certain circumstances:**
  - **to the patient, upon the patient's request, subject to exceptions**
  - **to the Secretary of DHHS to investigate or determine the provider's compliance with the privacy standards**

Covered Entity Obligations

- **A covered entity <u>may</u> disclose PHI for:**
  - **Treatment**
  - **Payment**
  - **Health care operations**

Covered Entity Obligations

- **Treatment:**
  - **the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another**

Covered Entity Obligations

- **Payment:**
  - **the activities undertaken by a health care provider to obtain or provide reimbursement for provision of health care and the activities related to the individual to whom health care is provided and include, but are not limited to, billing, claims management, collection activities, and related health care processing**

Covered Entity Obligations

- **Health Care Operations**
  - **conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment**
  - **reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, training of health care and non-health care professionals; accreditation, certification, licensing, or credentialing activities**
  - **conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs**
  - **business planning and development, general management activities of the entity, fundraising, and resolution of internal grievances**

Organized Health Care Arrangements

- **The Privacy Rule also permits a covered entity that is part of an *organized health care arrangement* to disclose protected health care information about an individual to another covered entity that participates in the arrangement for any health care operations of the organized health care arrangement**

- **HCAP and other provider networks may qualify as an organized health care arrangement depending on the functions of the network and how the network is organized and operated**

- **Covered entities that participate in an organized health care arrangement may disclose PHI to another covered entity participating in the arrangement for any health care operations of the organized health care arrangement**

Organized Health Care Arrangements

- **An organized health care arrangement is:**
  - **a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; or**
  - **an organized system of health care in which more than one covered entity participates, and in which the participating covered entities:**

    (1) hold themselves to the public as participating in a joint arrangement

    (2) participate in joint activities that include *at least one* of the following:

Organized Health Care Arrangements

- **utilization review in which health care decisions by participating entities are reviewed by other participants or by a third party on their behalf**
- **quality assessment and improvement activities, in which treatment provided by participating entities is assessed by other participating entities or by a third party on their behalf, or**
- **payment activities if the financial risk for delivering health care is shared, in part or in whole, by participating entities through the joint arrangement and if PHI created or received by a participating entity is reviewed by participants or by a third party on their behalf for the purpose of administering the sharing of financial risk**

Organized Health Care Arrangements

- **Covered entities participating in an organized health care arrangement may use a joint privacy notice, provided:**
  - **that the notice meets all of the requirements of the Privacy Rule, except for alterations reflecting the joint arrangement and it:**
    - **describes the participants and service sites to which the joint notice applies with reasonable specificity**
    - **states, if applicable, that the participants will share PHI with each other as necessary to carry out the payment, treatment, and health care operations of the arrangement, and**
  - **that all of the participants agree to abide by the terms of the notice with respect to PHI created or received as part of its participation in the arrangement**

- **The joint notice must be provided as required by the Privacy Rule, but provision by one participant will satisfy the requirements for all other participating covered entities**

"Minimum Necessary" Requirement

When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purposes of the use, disclosure, or request

Minimum necessary requirements do *not* apply to:

- **disclosures and requests among health care providers for treatment purposes**
- **permitted and required disclosures to a patient**
- **uses and disclosures made pursuant to a valid authorization**
- **uses and disclosures to federal authorities for enforcement purposes**
- **uses and disclosures required by law**
- **uses and disclosures required for compliance with regulations implementing HIPAA's other administrative simplification provisions**

Authorizations

An authorization is *not* needed:

- **to carry out treatment, payment or health care operations**
- **for releases authorized or required by law**
- **for disclosures to family, friends and others with the patient's oral agreement**

An authorization is needed for the use and disclosure of psychotherapy notes, except:

- **for treatment purposes by the professional who created the notes**
- **for certain covered entities' training programs**
- **to defend a legal action brought by the patient**
- **for releases authorized or required by law, for oversight of the originator of the notes, to avert a serious threat to health or safety of an individual, and to coroners and medical examiners**

A covered entity must provide a copy of the signed authorization to the patient if the covered entity requested the authorization (*e.g.*, for marketing or research purposes)

Authorizations

An authorization is required when, for example, the covered entity:

- **releases PHI to another health care provider or health plan for other than treatment, payment or health care operations**
- **uses PHI for fundraising purposes**
- **engages in certain marketing activities**
- **uses PHI in a clinical study**
- **receives a request for PHI from an attorney**

"Marketing" does not include:

- **a face-to-face communication between a member of the covered entity's workforce and a patient**
- **a promotional gift of nominal value provided by the covered entity**

Authorizations

To be valid, an authorization must:

- **be written in plain language**
- **include:**
  - **a description of the PHI to be used or disclosed, in a specific and meaningful fashion**
  - **certain information about the person authorized to use or disclose the PHI**
  - **certain information about the person to whom the PHI may be released**
  - **a description of each purpose of the use or disclosure or "at the request of"**
  - **an expiration date or event**
  - **the signature of the patient or personal representative (with authority) and the date of signature**

Authorizations

To be valid, an authorization must contain:

- **a statement and description of the patient's right to revoke, and how to do so, and exceptions thereto**
- **a statement that the covered entity cannot condition the provision of treatment on the provision of a signed authorization (unless research related or solely for disclosures to a third party)**
- **a statement that the information may be subject to re-disclosure and may no longer be protected by the covered entity's privacy practices and applicable privacy law**
- **if applicable, a statement that marketing activity involves direct or indirect remuneration to the covered entity**

Authorizations

Combining Authorizations

- Authorizations for different uses and disclosures may be combined into one document
- Authorizations relating to psychotherapy notes may not be combined with other authorizations
- Authorizations generally may not be combined with any other document
- Any use and disclosure must be consistent with the authorization

Authorizations

Revocation of Authorizations

A patient may revoke an authorization at any time. Revocation:

- must be in writing
- will not apply to the extent that action was taken in reliance on the patient's authorization

An authorization is defective if:

- it has expired
- it does not contain a required element
- it is known to have been revoked by the patient
- it was obtained in violation of the prohibition on conditioning treatment upon signing an authorization
- it was obtained in violation of the restriction on compound authorizations
- any material information in the authorization is known to be false

<u>Authorizations must be retained for six years</u>

Uses and Disclosures for Research Purposes

- **A covered entity may use or disclose PHI for research, regardless of the source of funding, provided that:**
  - **any alteration or waiver of the patient authorization to disclose PHI required by the Privacy Rule has been approved by either an Institutional Review Board (IRB) or a Privacy Board**
  - **the use or disclosure is sought solely for review to prepare a research protocol or for similar purposes preparatory to research, the information sought is necessary for research purposes, and no PHI will be removed from the covered entity**
  - **the use or disclosure sought is solely for research on the PHI of decedents, death has been documented, and the information sought is necessary for the research purposes**
- **The Privacy Rule requirements for IRB or Privacy Board modification of a patient authorization are rigorous. A covered entity participating in research involving protected heath information should review the Privacy Rule provisions carefully**

Disclosures Without Direct Identifiers

- **A covered entity may, for research, public health or health care operations, use or disclose a limited data set that meets the requirements of the Privacy Rule, if it enters into a data use agreement with the limited data set recipient**

- **A limited data set is PHI that excludes certain identifiers, such as the patient's name, address, telephone number, e-mail address, SSN, medical record numbers, *etc*.**

Disclosures Without Direct Identifiers

- **The covered entity must obtain satisfactory assurance (in the form of a data use agreement that meets the requirements of the Privacy Rule) that the limited data set recipient will only use or disclose the PHI for limited purposes**
- **A covered entity is not in compliance with the Privacy Rule if it knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation. Discontinuation of the disclosure or reporting the problem to the appropriate federal authorities may be necessary if the problem cannot be resolved**

De-identification

- **Information can be "de-identified" in two ways:**

  (1) A person "with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" determines that there is a "very small risk" that the information could be used alone, or with other reasonably available information, to identify an individual, or

  (2) Specific identifiers, *e.g.*, name, address, age, birth date, zip code, *etc.*, and any other unique characteristics are removed

- **The requirements for de-identification are set forth in 164.514(b). They are highly technical. Since release of PHI without a patient authorization or as otherwise permitted by the Privacy Rule would violate the rule, covered entities should not attempt to de-identify PHI without expert advice**

Business Associates

- **A covered entity may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf if the covered entity receives satisfactory assurance that the business associate will appropriately safeguard the information**

- **<u>Definition:</u> A business associate is a person or entity who performs, or assists in the performance of, a function or activity on behalf of the covered entity, when the function or activity involves the use or disclosure of individually identifiable health information. A member of the covered entity's workforce is not a business associate**

Business Associates

- **Typical business associate functions and activities include:**
  - **claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; and practice management**
  - **the provision of legal, accounting, actuarial, consulting, data aggregation, management, accreditation, administrative or financial services**
  - **any other function or activity regulated by the Privacy Rule**

- **A covered entity may be a business associate of another covered entity, *e.g.*, providing data processing, consulting, management services, *etc.***
- **The business associate standards do not apply to a disclosure by the covered entity to another health care provider concerning the treatment of an individual**

Business Associates

A covered entity is not required to monitor the activities of its business associates. However, the covered entity would violate the Privacy Rule if it knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligations under the contract, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful, terminate the contract or arrangement, if feasible, or, if not feasible, report the problem to DHHS

Business Associates

Security Provisions

- **A covered entity may permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information**
  - **The Security Rule does not apply with respect to the transmission by a covered entity of electronic PHI to a health care provider concerning treatment of an individual**
  - **A covered entity obtains satisfactory assurance only if there is a written contract with the business associate that provides that the business associate will:**

Business Associates

Security Provisions (continued)

(a) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the covered entity

(b) Ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it

(c) Report to the covered entity any security incident of which it becomes aware

(d) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract

These provisions are <u>in addition to</u> business associate contract provisions required under the HIPAA Privacy Rule.

Security Standard

- **The HIPAA Security Standard categorizes requirements into the following areas:**
  - **Administrative Safeguards to Guard Data Integrity, Confidentiality, and Availability**
  - **Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability**
  - **Technical Safeguards to Guard Data Integrity, Confidentiality, and Availability**
  - **Organizational Requirements**

Security Standard

- **"Required" versus "Addressable"**
  - **Certain specifications are required for all covered entities**
  - **Other specifications are addressable. This means that a covered entity must:**
    - **Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic PHI, and, as applicable:**
      - **Either implement the specification, and if this is not viable,**
      - **Document why it would not be reasonable and appropriate to do so, and implement an equivalent alternative measure if reasonable and appropriate**

Security Standard

Compliance Dates

- **The final security regulations were published in February 2003. Health care providers, health care clearinghouses and health plans have until April 21, 2005 to comply with the applicable requirements**

Security Standard

Administrative Safeguards

- **Security Management Process**
  - **Risk Analysis**
  - **Risk Management**
  - **Sanction Policy**
  - **Information System Activity Review**
- **Assigned Security Responsibility**
- **Workforce Security**
  - **Authorization and/or Supervision**
  - **Workforce Clearance Procedure**
  - **Termination Procedures**
- **Information Access Management**
  - **Isolating Health Care Clearinghouse Function**
  - **Access Authorization**
  - **Access Establishment and Modification**

Security Standard

Administrative Safeguards

- **Security Awareness and Training**
  - **Security Reminders**
  - **Protection from Malicious Software**
  - **Log-in Monitoring**
  - **Password Management**
- **Security Incident Procedures**
  - **Response and Reporting**
- **Contingency Plan**
  - **Data Backup Plan**
  - **Disaster Recovery Plan**
  - **Emergency Mode Operation Plan**
  - **Testing and Revision Procedure**
  - **Applications and Data Criticality Analysis**
- **Evaluation**
- **Business Contract and Other Arrangement**
  - **Written Contract or Other Arrangement**

Security Standard

Physical Safeguards

- **Facility Access Controls**
  - **Contingency Operations**
  - **Facility Security Plan**
  - **Access Control and Validation Procedures**
  - **Maintenance Records**
- **Workstation Use**
- **Workstation Security**
- **Device and Media Control**
  - **Disposal**
  - **Media Re-use**
  - **Accountability**
  - **Data Backup and Storage**

Security Standard

Technical Safeguards

- **Access Controls**
  - **Unique User Identification**
  - **Emergency Access Procedure**
  - **Automatic Logoff**
  - **Encryption and Decryption**
- **Audit Controls**
- **Integrity**
  - **Mechanism to Authenticate Electronic PHI**
- **Person or Entity Authentication**
- **Transmission Security**
  - **Integrity Controls**
  - **Encryption**

Organizational Requirements

- **Business Associate Contracts or Other Arrangements**

DHHS Compliance Principles

- **DHHS will, "to the extent practicable," seek the cooperation of covered entities in achieving compliance**

- **DHHS may provide technical assistance to help covered entities comply voluntarily with the Privacy Rule**